

Federal Aviation Administration's Information Systems Security Program

Michael F. Brown

Director
Information Systems Security
Federal Aviation Administration



The FAA's Job

Each day, manage 30,000 commercial flights to safely move 2,000,000 passengers

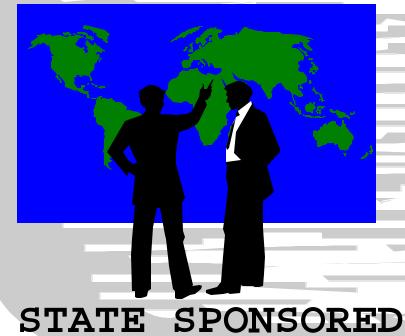


- ~ 500 FAA
 Managed Air
 Traffic Control
 Towers
- ~ 180 Terminal Radar Control Centers
- 20 Enroute Centers
- ~ 60 Flight
 Service Stations
- ~ 40,000 Radars,
 VORs, Radios,

. . .



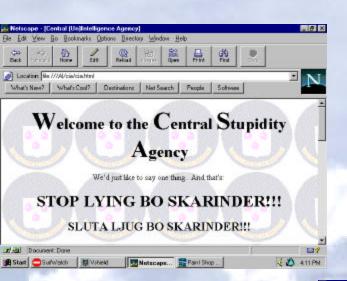
HACKERS





ORGANIZED CRIME

HACKED WWW HOMEPAGES



CIA HOMEPAGE



DOJ HOMEPAGE

United States

Department of

Netscape - [U. Paix Shop Pro 415PM

Injustice

USAF

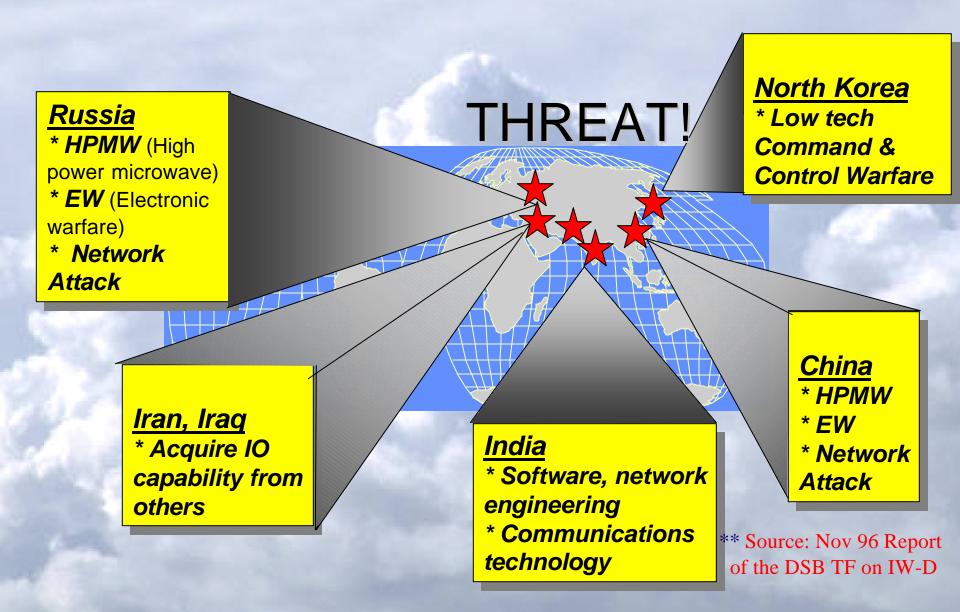
HOMEPAGE

What's New? | What's Cool? | Destinations | Net Search | People | Soltware

2 sal Document Done

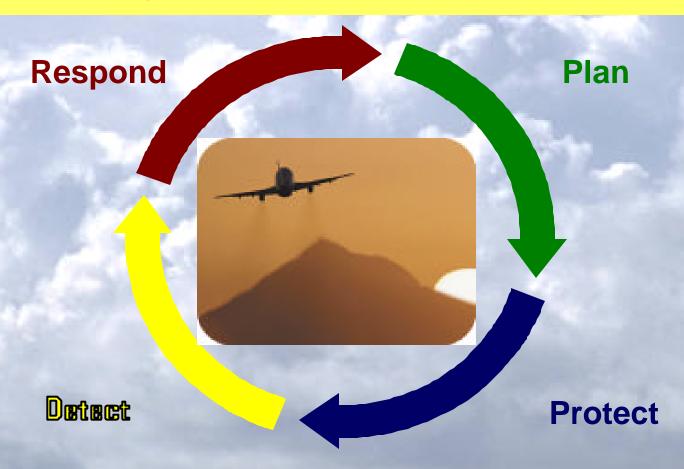
Start SurWalch

Information Operations Capabilities **

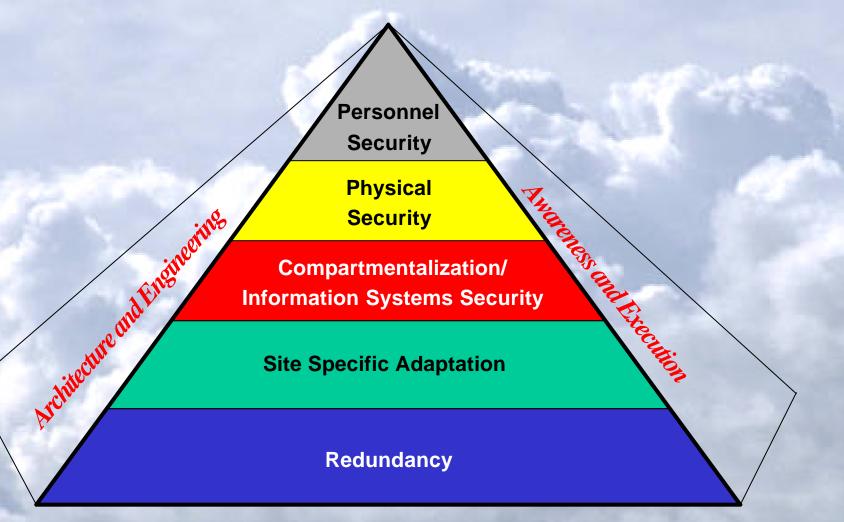


CIO's Security Mission

Protect the FAA's information infrastructure and help the aviation industry reduce security risks through leadership in innovative information assurance initiatives

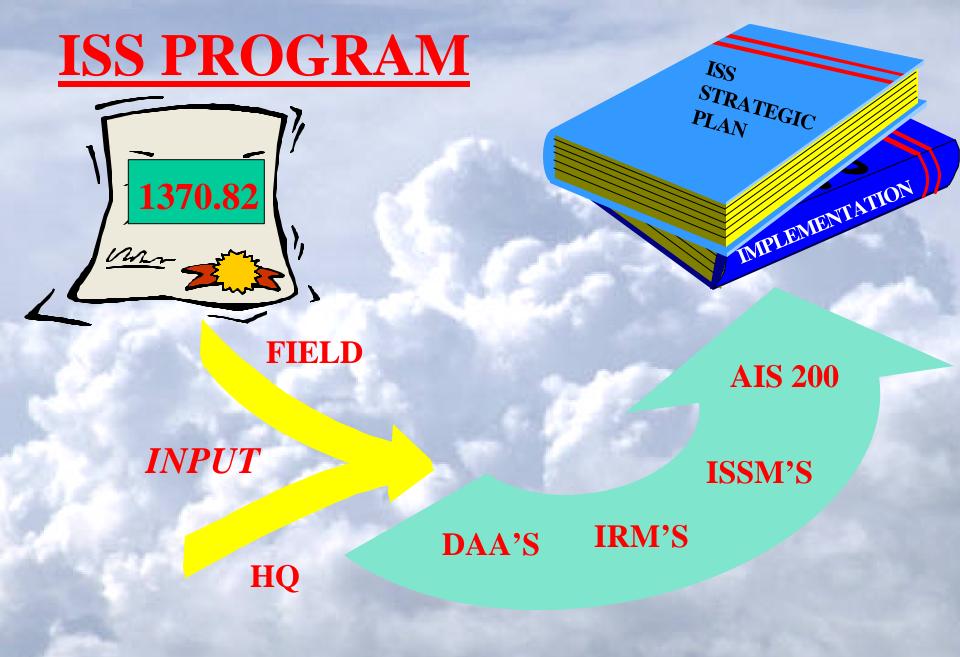


FAA's 5 Layers of System Protection

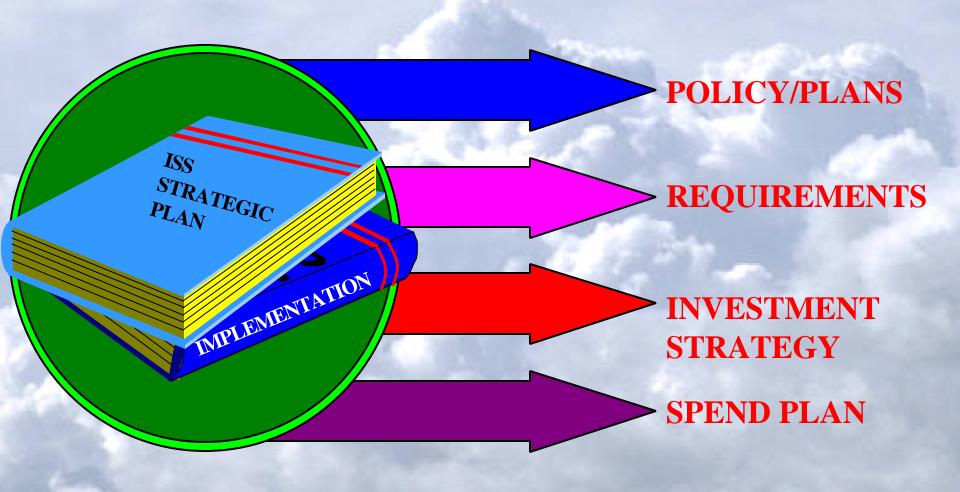


ISS Approach

- Establish a Centralized Program to Manage and Monitor Information System Security (ISS) Efforts.
- Implement a Comprehensive ISS
 Approach To Mitigate Security Risks.
- Implement a Computer Security Incident Response Capability (CSIRC) to Detect and Respond to Cyber Threats.
- Implement a Comprehensive Security Awareness & Training Program.
- Work Closely with Government and Private Sector Organizations.



ISS PROGRAM





INTERNET SERVICES



PASSWORDS

TRAINING/ AWARENESS



TRAININGAN INVESTMENT IN PEOPLE

GOALS:

- 60% OF 381 BY SEPT 01
- AWARENESS DAYS AT REGIONS & HQ

MTT TECHNICAL FORMAL WORKSHOPS AWARENESS TRAINING PLAN

Computer Based Training (CBT)

- Available Courses
 - Internet Security
 - Network Essentials: Data Security
 - Windows 98 Implementation & Support: Security
 - Novell NetWare 5 Administration:
 - File System Security Management
 - NDS Security Management
 - Solaris 2.5.1 System Administration: user Setup & Security
 - Internet & Intranet Skills: Web Site Security
- Source: FAA Academy
- Contact: www.academy.jccbi.gov

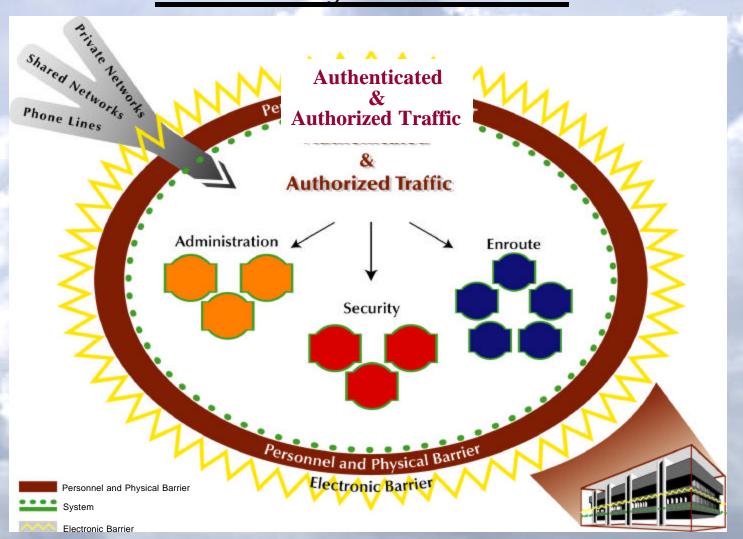
Computer Based Training (CBT)

- Upcoming Courses
 - Network Security for Windows 2000
 - Securing Local Area Networks (LAN)
 - Network Vulnerabilities and Prevention
 - Security Firewalls for E-commerce
 - Identifying Viruses
 - Troubleshooting LANs
 - Overview of Java Security
 - Encrypting File Systems
 - Security Over Internet Protocol
- Source: AIS Procured CBT Courses
- Contact: AIS-100, Natalie Miller, 202-267-9279

Classroom Training

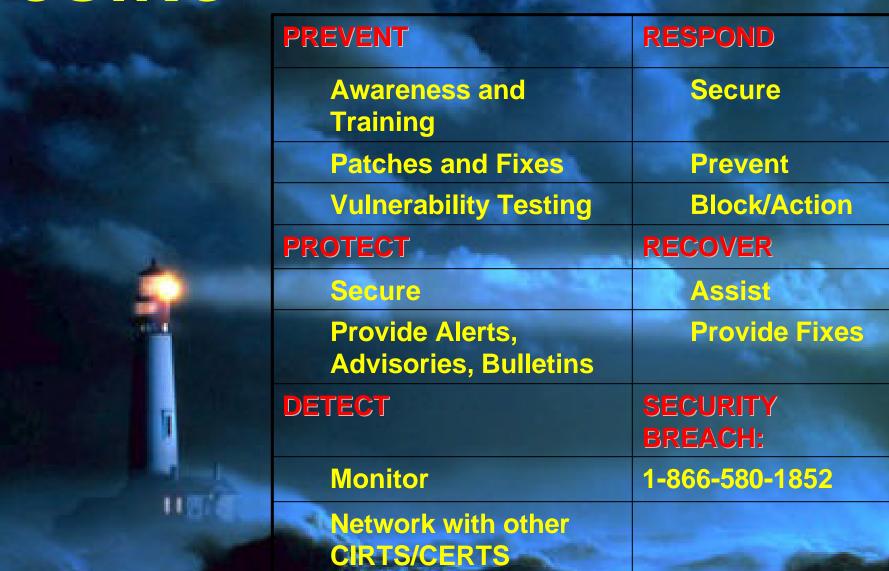
- ISSO
 - Threat
 - Risk Management
 - Network Security
 - Personnel Security
 - Access Control
 - Certification and Authorization Process
- Tentative Locations/Dates:
 - Washington DC August 6 and September 10, 2001
 - Oklahoma City August 20, 2001
 - Atlantic City, NJ September 24, 2001
- Contact: AIS-100, Natalie Miller, 202-267-9279

Integrated Facility Security IOC Boundary Protection

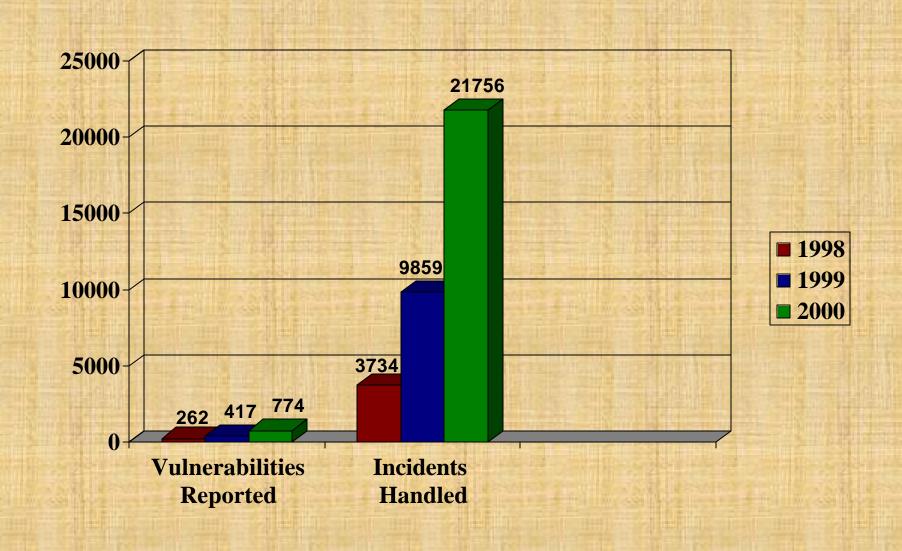




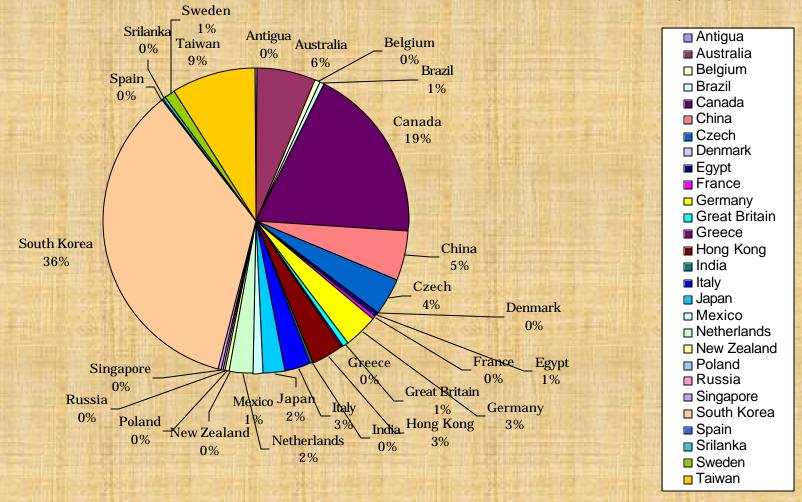
CSIRC



Exponential Growth in Security Incidents

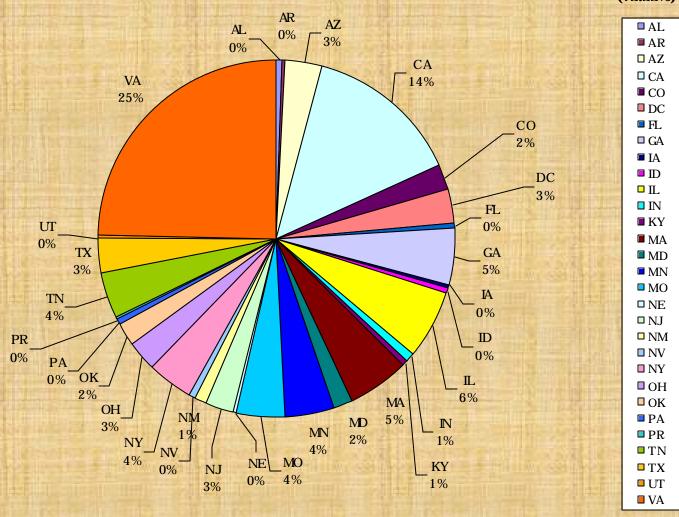


Trend Analysis - Foreign Attempts 1 NOV 00 - 20 Feb 01 (27.78%)



Trend Analysis - Domestic Attempts Attempts Domestic

DOMESTIC ATTEMPTS 1 NOV 00 - 20 Feb 01 (72.22%)



CSIRC Notification Process

Listserv utilized to accommodate Communities of Interest (COI)

- Web Administrators
- Network Administrators
- · ISSM/ISSO

CSIRC Notification and Tracking Database

- 5 days to acknowledge receipt
- 30 days to advise compliance

CSIRC Personnel

Current Status:

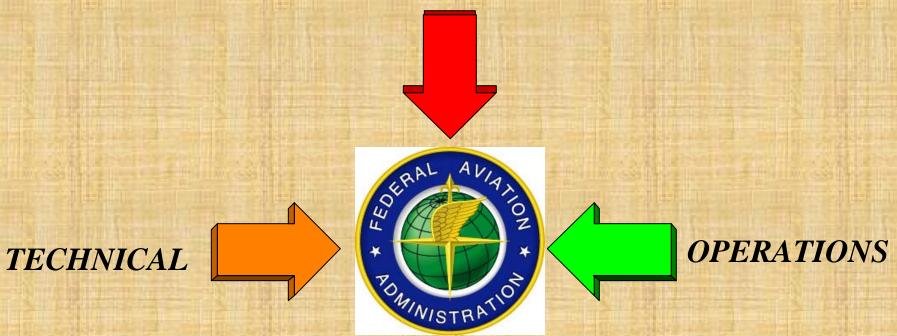
- Staffing one shift 5 X 8
- 3 government employees
- 6 CSC business partners

Future Plans:

- 2 shifts after October 1, 2001 5 X 16
- 3 shifts after April 1, 2002
 Minimum of 25 employees required -24 X 7

IN SUMMARY:

POLICY/PLANS/TRAINING



ISS PROGRAM

